RESEARCH PLAN PROPOSAL

Design and Development of a Framework for Dynamic Authentication in Mobile Ad Hoc Networks

For registration to the degree of
Doctor of Philosophy

IN THE FACULTY OF SCIENCE

THE IIS UNIVERSITY, JAIPUR

Submitted by

Priyanka Sogani
Enroll. No.: IISU/2012/10023
Roll No.: 127054

Under the Supervision of

Dr. Aman Jain
Professor & HOD (CS)
Deepshikha College of Technical Education, Jaipur

Department of Computer Science

May 2013

1. Topic

Design and Development of a Framework for Dynamic Authentication in Mobile Ad Hoc Networks

2. Introduction

A **mobile ad hoc network** (**MANET**) is a self-configuring infrastructure less network of mobile devices connected by wireless. *Ad hoc* means "for this purpose". Each device in a MANET is free to move separately in any direction, and will therefore change its links to other devices frequently. Each must forward traffic not related to its own use, and therefore each node become a router. Mobile ad hoc networks (MANETs) are one of the greatest growing areas of research. . They are an attractive technology for many applications, such as rescue and tactical operations, due to the flexibility provided by their dynamic infrastructure [1]. The basic structure of Mobile Ad-Hoc Network is shown in Fig 1.

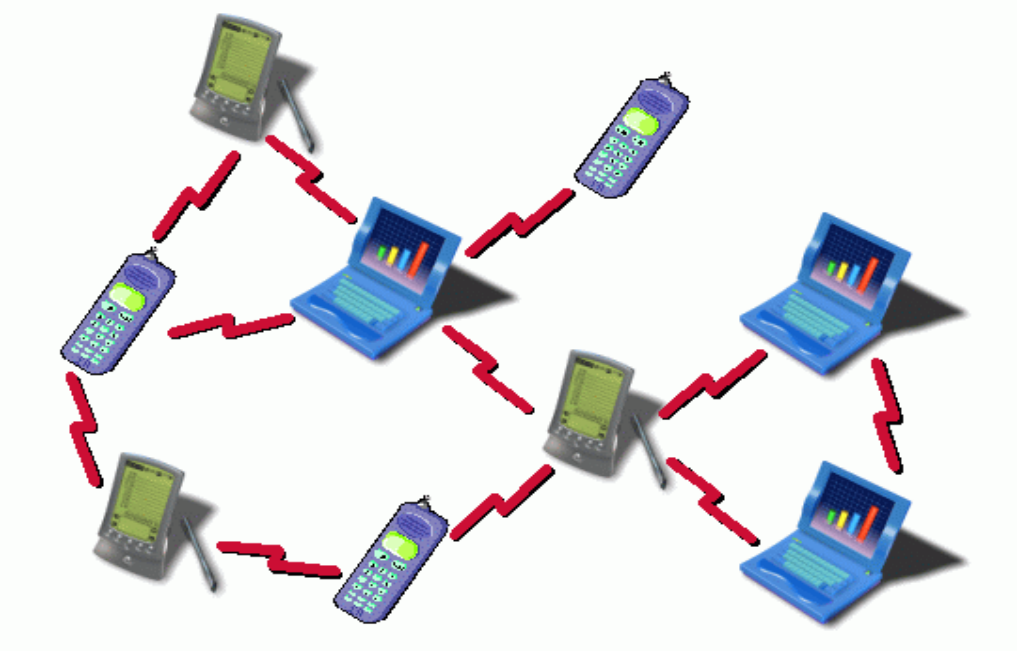


Fig. 1 Basic Structure of Mobile Ad-Hoc Network

Characteristics of MANET

- Dynamic Topologies: - Nodes are free to move randomly with different speeds; thus, the network topology may change randomly and at unpredictable times.
- Energy Constrained Operation: - Some or all of the nodes in an ad hoc network

may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design optimization criteria may be energy conservation.

- Limited Bandwidth: - Wireless links continue to have significantly lower capacity than infrastructured networks. In addition, the realized throughput of wireless communications – after accounting for the effects of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.
- Security Threats: - Mobile wireless networks are generally more prone to physical security threats than fixed- cable nets. The increased possibility of eavesdropping, spoofing, and minimization of denial-of-service type attacks should be carefully considered. [2]

3. Review of Literature

3.1 Introduction

Recent advances in portable computing and wireless technologies are opening up exciting potential for the future of wireless mobile networking. A Mobile Ad hoc Network (MANET) consists of movable platforms which are free to move arbitrarily. The flexibility of mobile ad hoc network introduces new security threats. Many conventional security solutions used for wired networks are ineffective and inefficient for the highly dynamic and resource-constrained environments where MANET use may be predictable. [13]

3.1.1 Security goals

In mobile ad hoc networks, all networking functions, such as routing and packet forwarding, are performed by the nodes themselves in a self-organizing manner. For this reason, such networks have increased vulnerability and securing a mobile ad hoc network is very demanding. The following attributes are essential issues related to mobile ad hoc networks, especially for security-sensitive applications [18]

- Availability: - This feature ensures the survivability of network services despite denial of service attack.

- Integrity: - This feature ensures that a message being transferred is never corrupted.
- Confidentiality: - This characteristic ensures that certain information is never disclosed to unauthorized entities.[19]
- Authentication: - This feature enables a node to ensure the identity of the peer node it is communicating with.
- Non-Repudiation:- This feature ensures that the origin of a message cannot deny having sent the message.[12]

3.2 History of Mobile Ad Hoc Network

The whole life-cycle of ad-hoc networks could be categorized into the first, second, and the third generation of ad-hoc networks systems. Current ad-hoc networks systems are considered the third generation.

The first generation goes back to 1972. At the time, they were called PRNET (Packet Radio Networks). In combination with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a type of distance-vector routing PRNET were used on a test basis to provide different networking capabilities in a battle environment.

The second generation of ad-hoc networks emerged in 1980s, when the ad-hoc network systems were further enhanced and implemented as a part of the SURAN (Survivable Adaptive Radio Networks) program. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure. This program proved to be beneficial in improving the radios' performance by making them smaller, cheaper, and resilient to electronic attacks.

In the 1990s, the concept of commercial ad-hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences.

3.3 Security Issues in Mobile Ad Hoc Networks - A Survey

In this paper, the researchers were tried to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the conventional wired networks. They introduce the basic characteristics of the mobile ad hoc network. However, with the convenience in establishing the mobile ad hoc network, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention. Some typical and risky vulnerability in the mobile ad hoc networks are also discussed in this paper, most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media and limited battery power. The existence of these vulnerabilities has made it compulsory to find some effective security solutions and protect the mobile ad hoc network from all kinds of security risks. The researcher discussed two kinds of well-liked security techniques in the mobile ad hoc network, which are intrusion detection techniques and secure routing techniques. In each of the security schemes, several specific methods are pointed out and compared with each other. On the basis of certain observations, some methods had been point out that can be further explored for their betterment. The researcher also focused on the security solutions in the mobile ad hoc networks. They analyze the main security criteria for the mobile ad hoc networks, which should be regarded as a guideline for them to find the solutions to the security issues in the mobile ad hoc networks. They also point out various attack types that mainly threaten the mobile ad hoc networks. According to these attack types, a survey had been done for several security schemes that can partly solve the security problems in the mobile ad hoc networks. During the review, they also find some points that can be further explored in the future, such as some aspects of the intrusion detection techniques can get further improved. [3]

3.4 Security Threats in Mobile Ad Hoc Network

Mobile Ad Hoc Networks have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Whether ad hoc networks have vast potential, still there are many challenges left to

overcome. Security is an important feature for deployment of MANET. In this paper, the challenges and solutions of the security threats in mobile ad hoc networks have been overviewed. The researchers identify the existent security threats an ad hoc network faces, the security services required to be achieved and the countermeasures for attacks in each layer. They have also done literature survey in gathering information related to various types of attacks and solutions, as well as identified the challenges and proposed solutions to overcome them. They focus on the findings and future works which may be interesting for the researchers like robust key management, trust based systems, data security in different layer etc. However, the complete security solution which requires the prevention, detection and reaction mechanisms for MANET is still to develop. Though significant research in MANET has been ongoing for many years, but still in an early stage. [4]

3.5 SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks

Security is a critical issue in a mobile ad hoc network (MANET). In this paper, the researchers propose and investigate a novel scheme, Security Protocol for Reliable Data Delivery (SPREAD), to enhance the data confidentiality service in a mobile ad hoc network. The proposed SPREAD scheme aims to provide further protection to secret messages from being compromised (or eavesdropped) when they are delivered across the insecure network. The basic idea of SPREAD is to distribute the secrecy, first by secret sharing algorithm at the source node and then by multi path routing while shares are delivered across the network, so that in the event that a small number of shares are compromised, the secret as a whole will not be compromised. They also investigate the major design issues of SPREAD idea. The simulation results show that SPREAD can provide more secure data transmission when messages are transmitted across the insecure network. In addition, they show that a redundant SPREAD scheme can be designed in such a way that a certain degree of reliability can be provided without sacrificing the security. A few remarks are in order. First, the SPREAD scheme considers the security when messages are transmitted across the network, assuming the source and destination are trusted. Secondly, the SPREAD scheme cannot address the confidentiality alone. It only statistically enhances such service. For example, it is still possible for adversaries to compromise all the shares, e.g. by collusion. Finally, the SPREAD can be made adaptive in the sense that the source node could make final decision whether a

message is delivered at certain time instant according to the security level and the availability of multiple paths. Moreover, the chosen set of multiple paths may be changed from time to time to avoid any potential capture of those multiple shares by adversaries. [5]

3.6 A Simple Encryption Keys Creation Scheme in Wireless Ad Hoc Networks

A mobile ad hoc network (MANET) is a collection of mobile nodes that temporarily integrate with each other to form a network. Such a network does not require the existence of a typical network infrastructure. There is no central entity with the authority to administer the services and configurations of the network. In this paper, the researchers propose the use of security mechanisms for MANETs that are designed based on the characteristics, functionalities, and goals of such networks. The aim is to initiate a paradigm shift in securing MANETs, in which the focus should be on building security solutions specifically developed for MANETs. For this purpose researchers introduced an encryption keys creation technique for MANETs based on the Diffie-Hellman key exchange. The technique is simple and preserves the ad hoc nature of MANETs. In this technique creating the key would require the exchange of just two messages (KC-Msg and KCR-Msg). It would also require each node to maintain a very simple data structure (the Keys Table KT). The Diffie-Hellman protocol is primarily subject to two types of attacks: brute force and man-in-the-middle attacks. In a brute force attack, an attacker may exhaustively try all possible keys to decrypt an encrypted message. In a man-in-the-middle attack, a third malicious entity presents itself as a legitimate entity in the protocol exchange. In future, a new protocol should be designed for authentication that follows the principle of ad hoc mobile networking. [6]

3.7 A Lightweight Authentication Protocol for Mobile Ad Hoc Networks

Traditional network authentication solutions rely on physically present, trust third-party servers, or called certificate authorities (CAs). Popular network authentication architectures include X.509 standard and Kerberos. However, ad hoc networks are infrastructure-less, and there is no centralized server for key managements. Hence traditional solutions do not meet the requirements of mobile ad hoc networks. The characteristics of mobile ad hoc networks (MANETs) determine that the authentication approaches to protect routing and data packet transmission in MANETs should be lightweight and scalable. In ad hoc networks, users need to assure the party who supposedly sent a message to another party is indeed the legitimate

party. Otherwise, a malicious node could tamper a network with forged data. These attacks can result in degraded performance of networks, interference of resource reservation, and unauthorized use of resources. To deal with these attacks, an authentication protocol needs to be in place to ensure that a packet is sent by an authentic and legitimate node. In this paper, the researchers propose a lightweight authentication protocol, which utilizes one-way hash chain to provide effective and efficient authentication for communications between neighboring nodes in MANETs. This protocol not only eliminates the high performance overhead imposed by asymmetric cryptography (such as digital signatures), but also avoids the difficulty of key management introduced by secret paired symmetric key. Our protocol also used delayed key disclosure to prevent a malicious entity from forging packets with Message Authentication Codes (MACs) with an already released key. The analysis shows that the protocol incurs low overhead penalty and achieves a low dropped packet rate on key disclosure. [7]

3.8 Review of Hashing as Security Tool in Wireless Ad Hoc Network

The study here proposes a theory in this paper based on Hashing as a tool. This scheme can make most of the on demand protocols secure. The study should help in making protocols more robust against attacks and standardize parameters for security in routing protocols. In ad hoc networks all nodes are responsible of running the network services meaning that every node also works as a router to forward the networks packets to their destination. It is very challenging for researchers to provide comprehensive security for ad hoc networks with the desired quality of service from all possible threats. Providing security becomes even more challenging when the participating nodes are mostly less powerful mobile devices. In this paper an effort has been made to evaluate various security designs proposed. The solution proposed stresses upon applying hashing techniques not only in prevention stage in the form of message and routing information authentication, but also in different stages of securing ad hoc networks. The efforts can be made in the direction of improving hash functions to avoid collisions, using stronger hash keys by making them dependent on additional parameters like biometric credentials, passwords, IP addresses etc. The hash techniques can also be tried for keeping the link status of the network. In this paper, the security threats for an ad hoc network has been analyzed and presented with the security objectives that need to be achieved. The paper

represents the first step of research to analyze the security threats, to understand the security requirements for ad hoc networks, and to identify existing techniques, as well as to propose new mechanisms to secure ad hoc networks. Hashing has been used as one of the tools. More skilled technical work has to be done to deploy these security mechanisms in an ad hoc network and to investigate the impact of these security mechanisms on the network performance. [16]

3.9 A Review of Previous Research Papers on Mobile Ad Hoc Network: Authenticating and securing End-to-End Communications through Encrypted key model for Mobile Ad Hoc Network

A MANET (Mobile Ad Hoc Network) is a communication network characterized by the absence of any fixed infrastructure. The combination of an ad hoc environment with multicast services induces new challenges towards the security infrastructure to enable acceptance and wide deployment of multicast communication. The most suitable solution to overcome these challenges is through establishment through data encryption model. This paper is focus on the design and analysis a security solution for Mobile ad – hoc Network (MANET) through the authentication data encryption model. The model is analyzed under various attacks and the result shows that the proposed model is highly resistant to attack in end to end communication. The End to End Communication in mobile ad-hoc networks are analyzed a security solution through the authentication data encryption model. The model is analyzed under Masquerade attacks, man in the middle attacks, Rollback attack attacks and Replay attacks and the result shows that the proposed model is highly resistant to attack in end to end communication. [17]

Limitations of the Previous Work

- There is no security solution which is present for the authentication of source and destination node in the SPREAD scheme.
- Most of the security mechanisms are not dynamic.
- The proper functioning of Intrusion Detection Technique is not yet defined.
- The overall Framework for authentication of nodes in Mobile Ad Hoc Networks is still to develop.

4. Motivation to the Work

Use of wireless links renders an Adhoc network vulnerable to link attacks ranging from passive eavesdropping to active impersonation, message replay and message deformation. Eavesdropping might give an attacker access to secret information thus violating confidentiality. Active attacks could range from deleting messages, injecting wrong messages; impersonate a node etc thus violating availability, integrity, authentication and non-repudiation. Nodes roaming freely in an unfriendly environment with relatively poor physical protection have non-negligible probability of being compromised. The point to be taken care in future research is to consider malicious attacks not only from outside but also from within the network from compromised nodes. For high survivability Adhoc networks should have a distributed architecture with no central entities, centrality increases vulnerability. Ad-hoc network is dynamic due to frequent changes in topology. Even the trust relationships among individual nodes also changes, especially when some nodes are found to be compromised. Due to inherent limitations in Mobile Ad Hoc Network, security is an area where lots of research work is to be taken place and the complete and dynamic security mechanism is still under research work. Now, the requirement is that the Security mechanism need to be on the fly (dynamic) and not static and should be scalable. Therefore a framework is required which gives a completely dynamic secured Mobile Ad Hoc Network. These limitations and the requirement of such a framework, gives motivation towards developing a mechanism for securing Mobile Ad Hoc Networks.

5. Objectives

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wire line networks, the unique characteristics of mobile ad hoc networks pose a number of challenges to security design. These challenges clearly make a case for building multifence security solutions that achieve both protection and desirable network performance. The development of mobile ad hoc network raises many key challenges. Among them security is one of the problem.

1. The goal of this research is to study the various factors affecting the security of Mobile Ad Hoc Networks.
2. A Comparative study of frameworks for authentication in mobile ad hoc networks.
3. A framework would be design and developed to achieve the dynamic authentication in Mobile Ad Hoc networks.

6. Plan of Work and Methodology:

Work Plan (Including Gantt chart):

For the first 6-7 Months: *In depth study on existing applications of Mobile Ad-Hoc Networks.*

Description: At the end of this step, we will have a good knowledge of mobile ad-hoc networks and the existing solutions for the security issue and also know about different challenges of this issue.

Document: Description of existing agendas while pointing out for each one the benefits and the drawbacks.

7-8 months for: *Comparative study of the frameworks for authentication in mobile ad hoc network.*

Description:- During this step, we will study about the different frameworks available for authentication in mobile ad hoc networks and compare their functionalities.

Document:- Description of existing frameworks with their benefits and drawbacks.

At least 10-12 months are required for: *Proposing a framework for implementing authentication in mobile ad-hoc networks.*

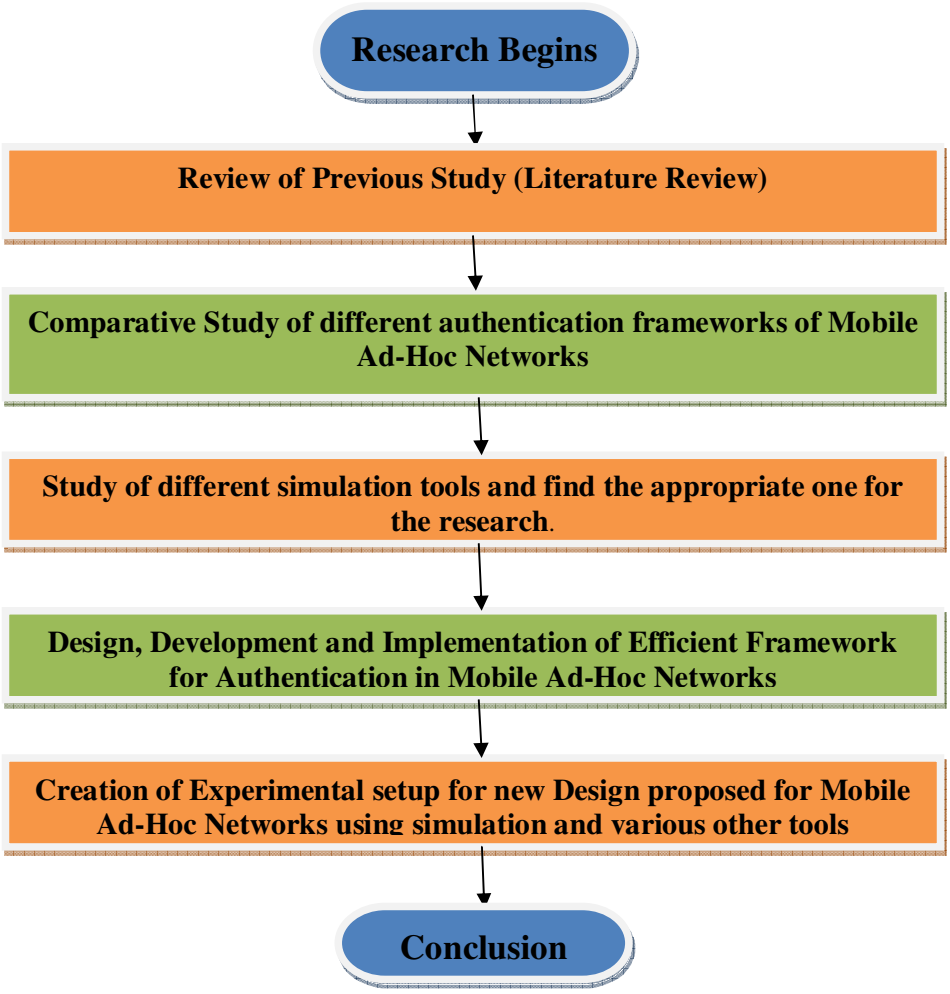
Description: During this step, we will focus on how different authentication issues effects the mobile ad hoc network and the result will be generated on the basis of simulation tools or/and real platform and test the framework. At the end of this step, we would be able to show a demonstration of the work done.

Document: Mainly a description of the proposed framework as well as difficulties and solutions to implement the authentication in MANETs.

5-6 months for: Documentation and thesis report writing

Methodology & Tools to be used:

Methodology


Research Begins
Review of Previous Study (Literature Review)
Comparative Study of different authentication frameworks of Mobile Ad-Hoc Networks
Study of different simulation tools and find the appropriate one for the research.
Design, Development and Implementation of Efficient Framework for Authentication in Mobile Ad-Hoc Networks
Creation of Experimental setup for new Design proposed for Mobile Ad-Hoc Networks using simulation and various other tools
Conclusion

- Different approaches can be considered to implement the security in mobile ad hoc networks.
- For this purpose, these are the following **tools** that can be used:

OPNET: - OPNET (Optimized Network Engineering Tools) is a commercial tool from OPNET Technologies for modeling and simulation of communications networks, devices, and protocols. It features graphical editors and animation. It has being developed for almost 15 years. It is widely held to be the state-of-the-art in network simulation. OPNET is used by large companies. OPNET is a well-established and highly professional product. OPNET, differently from NS-2 and GloMoSim, results quite easy to describe an application that bypasses part of the protocol stack. This aspect can be quite important to speed up and/or to reduce the level of unnecessary detail during the simulations. [8]

GloMoSim/QualNet: - GloMoSim is a scalable simulation library designed at UCLA Computing Laboratory to support studies of large-scale network models, up to millions of nodes, using parallel and/or distributed execution on a diverse set of parallel computers (with both distributed and shared memory). It has been designed for wireless and wired networks systems, but it currently supports only protocols for purely wireless networks. GloMoSim is a library for the C-based parallel discrete-event simulation language PARSEC. GloMoSim has several nice features. It comes with a rich suite of models, it is the only simulator among the considered ones that seems able to scale up to thousands of nodes, and its highly modular design is such that it appears quite straightforward to modify and/or extend the basic functionalities. GloMoSim is likely the second most used simulator, after NS-2, in the research community. Therefore, it is widely accepted from a scientific point of view. QualNet is based on GloMoSim but it dramatically expands its capabilities in terms of contributed models and protocols, graphical tools for experiment planning, analysis and visualization, as well as, in terms of available documentation and technical support. QualNet supports also some form of network emulation and allows designing realistic 3D environments. Basically, QualNet is quite complete as a simulator. [8]

NS-2:- NS-2 is the most popular simulator used in the research field of mobile ad hoc networks. NS-2 comes fully equipped of protocols, models, algorithms and accessory tools, and it is for free. Therefore, in terms of scientific acceptance, number of tools/modules and cost, NS-2 would be a sort of ideal choice. On the other hand, from the short given description of its architecture, it is quite clear that NS-2 is a rather complex software. Moreover, there is a lack of graphical tools that could greatly help code development. Unfortunately, the provided documentation does not help from this point of view. In fact, it is often limited and out of date with the current release of the simulator. A more troublesome limitation of NS-2 is its large memory footprint and its lack of scalability as soon as simulations of a few hundred to a few thousand of nodes are undertaken. [8]

OMNeT++:- The overall design of OMNeT++ is pretty nice and fully based on the driving ideas of object oriented design. In this respect, OMNeT++ is probably the best software product among the considered ones. The use of the simulator, as well as the definition of new custom models and protocols is quite easy when compared to the other simulators and to NS-2 in particular. Moreover, the nice graphical interface offers good potentialities for monitoring and analysis of the simulations. Unfortunately, some important network specific models and protocols are definitely missing. This fact, in spite of some interest that OMNeT++ is widely attracting, dramatically limits the use of OMNeT++. [8]

8. Place of Work and Facilities Available

The research work will be undertaken in the Laboratories available in the university campus and the software's and hardware's provided will be used as a part of the research work.

9. Limitations & Alternative Plan of the study

Some experiments and consultation may be required for the research work. Different labs may be used as per the requirement of the research.

10. Paper Presented:-

1) Presented a research paper titled "Security Issues and Challenges in Mobile Ad Hoc Networks." in the National Conference on Management and Information Technology, held on 12th and 13th April 2013.

11. References

[1] Djenouri, Djamel, L. Khelladi, and N. Badache "A Survey of Security Issues in Mobile Ad Hoc Networks", IEEE communications surveys Vol. 7, no. 4 (2005).

[2] De Morais Cordeiro, Carlos, and Dharma P. Agrawal "Mobile Ad Hoc Networking" Center for Distributed and Mobile Computing, ECECS, University of Cincinnati (2002).

[3] Li, Wenjia, and Anupam Joshi. "Security Issues in Mobile Ad Hoc Networks-A Survey" Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County (2007).

[4] Anuj Joshi1, Pallavi Srivastava, Poonam Singh, "Security Threats in Mobile Ad Hoc Network", S-JPSET: ISSN: 2229-7111, Vol. 1, Issue 2, Samriddhi, 2010.

[5] Wenjing Lou, Wei Liu Yuguang Fang, "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks", INFOCOM, 2004, IEEE, 2004.

[6] Altalhi, Abdulrahman H. "A Simple Encryption Keys Creation Scheme in Wireless Ad Hoc Networks" Communications and Network 4, no. 1 (2012).

[7] Lu, Bin, and Udo W. Pooch. "A Lightweight Authentication Protocol for Mobile Ad Hoc Networks" In Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on, vol. 2, pp. 546-551. IEEE, 2005.

[8] Di Caro, Gianni A. "Analysis of Simulation Environments For Mobile Ad Hoc Networks." Dalle Molle Institute for Artificial Intelligence, Tech. Rep (2003).

[9] Corson, M. Scott, Joseph P. Macker, and Gregory H. Cirincione., "Internet-Based Mobile Ad Hoc Networking" Internet Computing, IEEE 3, no. 4 (1999): 63-70.

[10] Michiardi, Pietro, and Refik Molva. "Ad Hoc Networks Security.", In ST Journal of System Research, 2003.

[11] Yang, Hao, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. "Security in Mobile ad Hoc Networks: Challenges and Solutions." Wireless Communications, IEEE 11, no. 1 (2004): 38-47.

[12] Moses, G. Jose, P. Suresh Varma, N. Supriya, and G. NagaSatish. "Security Aspects and Challenges in Mobile Adhoc Networks" International Journal of Computer Network and Information Security (IJCNIS) 4, no. 6 (2012): 26.

[13] Singh, Karan, and Rama Shankar Yadav. "A Review Paper on Ad Hoc Network Security" International Journal of Computer Science and Security (IJCSS) 1, no. 1 (2007): 52.

[14] Wen, Hsiang-An, Chun-Li Lin, and Tzonelih Hwang. "Provably Secure Authenticated Key Exchange Protocols for Low Power Computing Clients" Computers & Security 25, no. 2 (2006): 106-113.

[15] Garg, Nishu, and R. P. Mahapatra. "MANET Security Issues" International Journal of Computer Science and Network Security 9, no. 8 (2009): 241.

[16] Madan, Vikas, and Ashwani Kush. "Review of Hashing as Security Tool in Wireless Ad Hoc Networks", 2009

[17] Krishnan, Mukesh. "Authenticating and Securing End-To-End Communications Through Encrypted Key Model for Mobile Ad Hoc Network" International Journal of Computer Applications 35, no. 7 (2011).

[18] Lou, Wengjing, and Yuguang Fang. "A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions" Ad Hoc Wireless Networks (2003): 319-364.

[19] Novales, Ramon, and Neeraj Mittal. "Parameterized Key Assignment for Confidential Communication in Wireless Networks" Ad Hoc Networks 9, no. 7 (2011): 1186-1201.

[20] Ngai, Edith CH, Michael R. Lyu, and Roland T. Chin, "An Authentication Service Against Dishonest Users in Mobile Ad Hoc Networks" In *Aerospace Conference, 2004, Proceedings 2004 IEEE*, vol. 2, pp. 1275-1285, IEEE, 2004.